Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 314 – 322

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

The Impact Assessment of IT Infrastructure on Information Security: A Survey Report

Ankur Kumar Shrivastava

Research Scolar Sai Nath University,Ranchi,Jharkhand 834001,India

Abstract

Information technology infrastructure trigger unending concern for IT players accountable for information security. Sensitive organization information can be easily acquired and lost. The community dearth of self-confidence in information technology (IT) infrastructure is not purely about security of worth, but also about faith in the information group. Integrity, privacy and vulnerability security fears are the important cause web user is not confident over the web. Proposes to investigate the integrity, privacy and vulnerability security fears of IT user in order to establish a consensus among them. Uses data from 127 contributors to come to a decision that the following major concerns (in the descending of importance) exist: integrity, privacy, security and fears, unauthorized access, data leaked, impersonation and forged identity and e-mail safety. The objective of the survey was to collect statistics to quantify the influence of Information technology infrastructure on organization information security.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: Risk assessment; Threat evaluation; Risk gauge: Quantitative; Qualitative; Privacy; Integrity; Vulnerability.

1. Introduction

The establishments in the private and public segments rely on information classifications to positively carry out their duties and commercial roles. Information technology infrastructure can include very distinct units varying from financial, office networks, and personnel systems to very specialized systems. IT infrastructure are question to risky hazards that can have negative effects on organizational processes, organizational assets, other organizations, individuals, and the Nation by utilizing both unknown and known vulnerabilities to compromise the integrity,

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.062

confidentiality, or availability of the information being managed, collected, or communicated by those systems. Risks to information and information systems can include persistent attacks, environmental disruptions, and man/machine errors and result in great damage to the national and economic security interests. Hence, it is essential that managers and leaders at all stages identify their duties and are held responsible for handling information security risk that is, the hazard associated with the process and use of information systems that support the processes and business functions of their organizations. Threat is a degree of the extent to which an entity is vulnerable by a potential incident or event, and is typically a function of: (i) the unfavorable effects that would arise if the situation or event occurs; and (ii) the probability of existence. Information security threats are those threats that arise from the loss of confidentiality, integrity, availability of information/information systems and expose the potential unfavorable impacts to organizational assets, organizational functions, individuals, other organizations, and the Nation. A risk measurement is the process of identifying, prioritizing, and evaluating information security risks. Evaluating information security danger requires the watchful examination of threat and vulnerability information to determine the extent to which situations or events could unfavorably impact an organization and the likelihood that such situations or events will occur. Any assessment of risk includes: (i) an precise risk model, outlining key terms and measureable risk factors and the associations among the factors; (ii) an evaluation approach, indicating the extent of values those risk factors can assume during the evaluations; and (iii) an evaluation approach, specifying how values of those threat factors are functionally merged to evaluate risk. Risk factors are characteristics used in risk models as inputs to determining levels of risk in risk assessments. Risk features are also used extensively in risk communications to focus the numerous features of problem domains that powerfully affect the intensities of risk in particular circumstances, situations, or contexts. Some of the risk factors include, for example, impact, threat, vulnerability, likelihood, and predisposing condition. Risk factors can be further decomposed into more detailed characteristics. A risk assessment methodology is a process for risk assessment, together with a risk model, assessment approach, and analysis approach. Risk evaluation practices are defined by organizations and are a factor of the risk management approach developed during the risk-framing step of the risk management procedure. Organizations can use a single risk evaluation procedure or can employ multiple risk evaluation procedures, with the selection of a specific practice depending on: (i) the criticality and sensitivity of the organization's core duties and business tasks including the supportive mission/business processes and information systems; (ii) the maturity of the organization's mission/business procedures; (iii) the stage of information systems in the SDLC. By making explicit the risk model, the assessment approach, and the analysis approach used, and requiring as part of the assessment process, a basis for the evaluated values of threat factors, organizations can increase the duplicability and reappearance of their threat evaluations.

1.1. Security Risk Models

This describes the crucial terms used in risk evaluations involving the factors of the risk to be evaluated and the associations among those factors. These explanations are vital for corporations to document previous of managing risk evaluations because the evaluations depend upon significant properties of threats, vulnerabilities, and other risk factors to well determine the risks. Figure 1. (a) Explains a pattern of a risk model for severe threats including the key risk factors related with the model and the association among the features. All of the risk factors is defined in larger detail underneath and used in the process of risk evaluation. A threat is an event with the potential to negatively impact organizational resources and processes, individuals, other organizations, or the Nation through information system via unlawful access, devastation, admission, or information modification, and/or denial of service. There are two sides to threat cogitated in this paper: (i) threat causes; and (ii) threat incidents. A threat cause is a play-actor with the intent and method targeted at the exploitation of vulnerability or a state and method that may unintentionally exploit vulnerability. In common, types of threat causes include: (i) adverse cyber/physical attacks; (ii) humanoid mistakes of exclusion or instruction; (iii) structural failures of organization-controlled resources; and (iv) natural and man-made adversities, mishaps, and flops beyond the control of the organization. A threat incident is an incident or condition initiated or caused by a threat cause that has the potential for causing adverse impact. The tactics, techniques, for cyber attacks typically characterizes threat events and procedures employed by adversaries. Risk models can provide useful differences between threat causes and threat incidents. Various taxonomies of threat causes have been established. A typical classification of threat causes uses the type of adverse impacts as an

establishing principle. Several threat causes can initiate or cause the same threat event for example, a key provisioning server can be taken down by a denial-of-service attack, a thoughtful act by a malicious system administrator, an administrative error, a hardware blunder, or a power breakdown. Risk models vary in the degree of detail and complexity with which threat events are identified. When threat incidents are recognized with great specificity, threat scenarios can be modeled and analyzed.

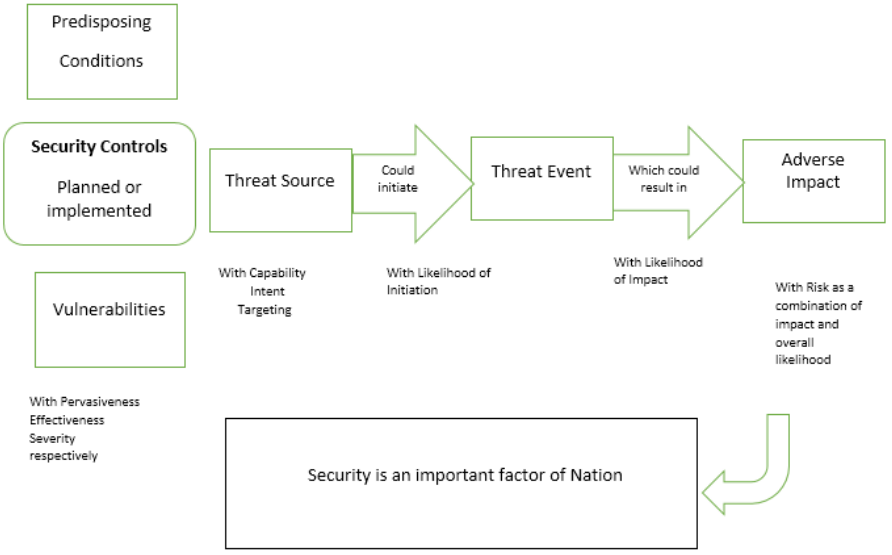


Fig. 1. (a) Risk Model

1.2. Assessment Approaches

Risk, and its causative features, can be evaluated in a variety of ways, involving qualitatively, quantitatively, or semi-quantitatively. Each risk assessment approach considered by organizations has merit and demerit. A required approach or circumstances-specified set of methods can be chosen based on corporate environment and, in specific, toward the ideas of uncertainty and risk communication. Quantitative assessment naturally engage a set of methodologies, principles, and rules for assessing threat based on the use of numbers where the meanings and proportionality of values are maintained internal and external the context of the assessment. This type of assessment best effectively supports cost benefit examines of unconventional risk responses or courses of action. However, the implication of the quantitative results may not always be perfect and may require a qualitative study. For example, organizations may ask if the statistics obtained in the risk assessment are good or poor or if the differences in the obtained values are insignificant. Additionally, the precision of quantification is considerably reduced when subjective determinations are suppressed within the quantitative assessments, or when meaningful insecurity surrounds the determination of values. The advantages of quantitative assessments (in terms of the precision, repeatability, and reproducibility of evaluation outcomes) can, in some cases, be outweighed by the price in relations of the experienced time and effort and the possible deployment and use of instruments required to make such assessments.

In compare to quantitative evaluations, qualitative evaluations normally use a set of actions, values, or rules for evaluating risk formed on non -statistical categories or notches example, very low, low, moderate, high, very high. This kind of assessment provisions to a much advanced level, threat communication in delivering evaluation results to resolution producers. Nevertheless, the choice of controls in qualitative evaluations is moderately little in maximum cases, creating the comparative prioritization or evaluation with in the set of specified risks challenging.

Furthermore, without each value is precisely outlined and is illustrated by expressive examples, unlike specialists trusting on their distinct experiences could produce considerably distinctive evaluation results. The reproducibility and repeatability of qualitative assessments are enhanced by the explanation of assessed values and by using tables or other well-defined functions to combine qualitative values.

Ultimately, semi-quantitative evaluations typically employ a set of actions, values, or guidelines for measuring threat that uses scales, bins, or representative numbers whose values and meanings are not preserved in added contexts. This assessment type can provide the benefits of both quantitative and qualitative assessments. The bins such as 0-10, 10-20, 20-30, 30-70, 71-85, 86-100 or gauges (e.g., 1-10) interpret easily into qualitative footings that support risk communications for decision makers (example, a result of 95 can be construed as very high), while also agreeing relative assessments between values in diverse bins or even within the same bin example, the difference between risks scored 70 and 71 correspondingly is quite irrelevant, while the distinction among risks scored 30 and 70 is relatively significant. The role of expert judgment in allocating values is more evident than in a simply quantitative method. Moreover, if the scales or sets of bins provide appropriate granularity, comparative prioritization among outcomes is better supported than in a purely qualitative approach. As in a quantitative method, consistency is noticeably minimized when subjective determinations are buried within assessments, or when significant uncertainty surrounds a determination of value. As with the non-numeric categories or stages used in a justifiable qualitative approach, each bin or range of values needs to be visibly defined and/or categorized by substantial examples.

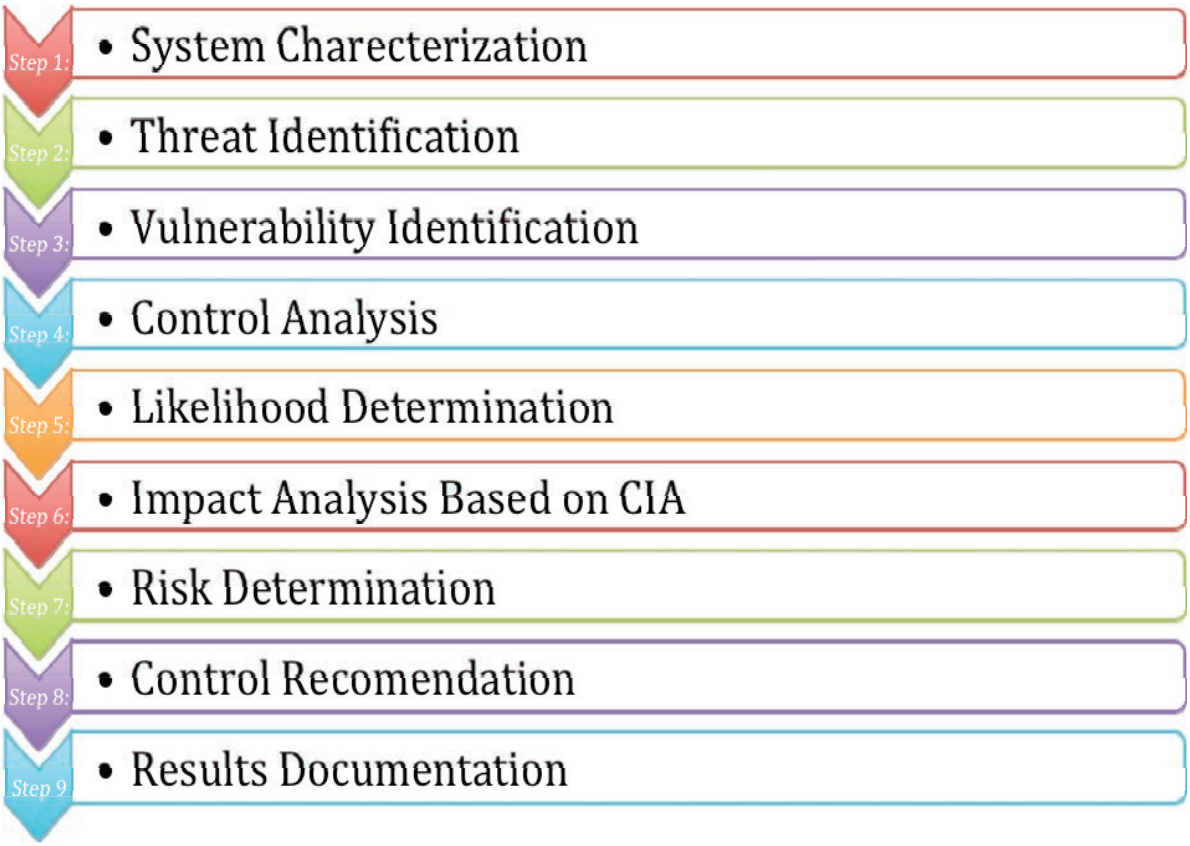


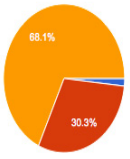
Fig. 1. (b) Risk Assessment Approach

2. Method of survey

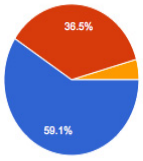
The purpose of this survey was to investigate the concerns of IT users in order to confirm or disconfirm the widely reported concerns in the press and trade journals. Reviewing the literature on the issue identified the different concerns as reported in this paper. A 34-item questionnaire was divided into 5 sections and mailed to 190 IT infrastructure users in a major city in INDIA. The items were derived from the privacy, integrity, vulnerability, security issues, news and other literature. The purpose of each of the items on the survey instrument was to give the IT users the chance to express their views and observations regarding their perception and concerns when using IT infrastructure. The items were naive declarations of interests for which the participants were asked to indicate their opinions on a scale of` "Not important to most important". The data used in the study come from the 127 useable responses (out of 190questionnaires), which is 66.8 percent of the total instrument sent out. Based on the demographics of those who participated in the study, there is no reason to trust that persons who did not respond the survey instrument are unlike from those who did. Simple illustrative statistics were acquired from the numbers and are discussed below.

3. Survey results

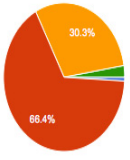
According to the statistical data, out of 127 individuals surveyed, 34.2 percentages were software personnel, 9.5 percentages were managers, consultant or supervisors; 16 percentages were faculty members; 25.1 percentages were undergraduates; and 15.8 percentages were others. More than 97 percentages people know the importance of security guards, visitor register and cctv camera however approx. 3 percent people consider it either least important or not important. Approx. 19 percentages are admitted that the biometrics access control is not important or least important for IT infrastructure information security. About 92 percentages people are admitted that their organization require an adequate security assessment policy. More than 11 percentages told that they don't think labeling and listing of hardware inventory across the organization is necessary. Up to 93 percentages admitted that there should be a separate id card for vendor and supplier to enhance the security. More than 96 percentages response is in favor of using license software and application. According to survey response more than 94 percentages agree that there must be a backup security policy in organization however more than 14 percentages are not aware with BCP plan. Almost 95 percentages are agreeing on strict network security policy and mechanism of IT infrastructure for their personal data security. More than 10 percentages respondent is unaware with procedure of change management and its impact.



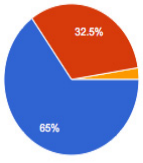
Senior management level	2	1.7%
Middle management level	36	30.3%
Junior management level	81	68.1%



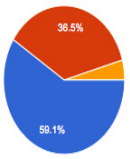
Less than 5 year	68	59.1%
5 to 10 year	42	36.5%
11 to 15 year	5	4.3%
More than 15 year	0	0%



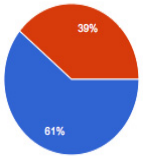
Diploma	1	0.8%
Graduate	79	66.4%
Post graduate	36	30.3%
Doctorate	3	2.5%



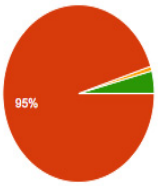
Below 30 year	78	65%
30 to 39 year	39	32.5%
40 to 49 year	3	2.5%
50 year and above	0	0%



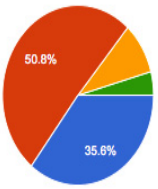
Less than 5 year	68	59.1%
5 to 10 year	42	36.5%
11 to 15 year	5	4.3%
More than 15 year	0	0%



Male	72	61%
Female	46	39%

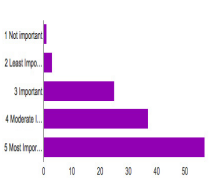


Government	0	0%
Private	115	95%
Public sector	1	0.8%
Other:	5	4.1%



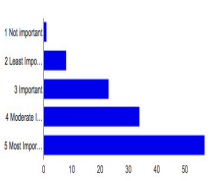
Large scale	42	35.6%
Medium scale	60	50.8%
Small scale	11	9.3%
Other:	5	4.2%

Importance of fire detection and suppression system for server rooms and building infrastructure [Section B - Physical Security of IT Infrastructure]



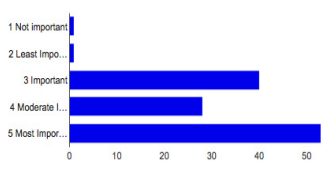
1 Not important	1	0.8%
2 Least Important	3	2.4%
3 Important	25	20.3%
4 Moderate Important	37	30.1%
5 Most Important	57	46.3%

Focus of organization on emergency exit [Section B - Physical Security of IT Infrastructure]



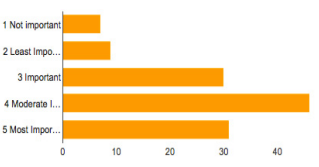
1 Not important	1	0.8%
2 Least Important	8	6.6%
3 Important	23	18.7%
4 Moderate Important	34	27.6%
5 Most Important	57	46.3%

Presence of security guards [Section B - Physical Security of IT Infrastructure]



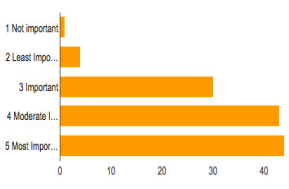
1 Not important	1	0.8%
2 Least Important	1	0.8%
3 Important	40	32.5%
4 Moderate Important	28	22.8%
5 Most Important	53	43.1%

Necessity of smoke detectors [Section B - Physical Security of IT Infrastructure]



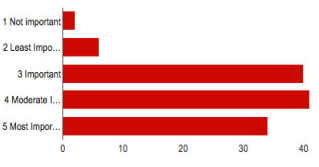
1 Not important	7	5.7%
2 Least Important	9	7.3%
3 Important	30	24.4%
4 Moderate Important	46	37.4%
5 Most Important	31	25.2%

Maintenance of visitor's information by security guards. [Section B - Physical Security of IT Infrastructure]



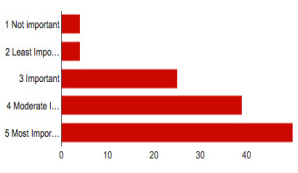
1 Not important	1	0.8%
2 Least Important	4	3.3%
3 Important	30	24.6%
4 Moderate Important	43	35.2%
5 Most Important	44	36.1%

Requirement of adequate security assessment [Section B - Physical Security of IT Infrastructure]



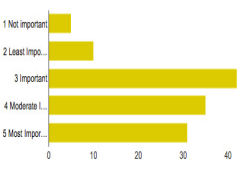
1 Not important	2	1.6%
2 Least Important	6	4.9%
3 Important	40	32.5%
4 Moderate Important	41	33.3%
5 Most Important	34	27.6%

Requirement of CCTV cameras installation [Section B - Physical Security of IT Infrastructure]



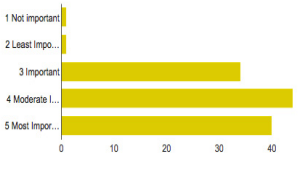
1 Not important	4	3.3%
2 Least Important	4	3.3%
3 Important	25	20.5%
4 Moderate Important	39	32%
5 Most Important	50	41%

Requirement of mock drill for known threats [Section B - Physical Security of IT Infrastructure]



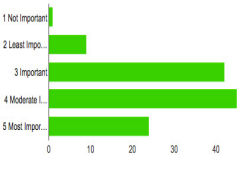
1 Not important	5	4.1%
2 Least Important	10	8.1%
3 Important	42	34.1%
4 Moderate Important	35	28.5%
5 Most Important	31	25.2%

Requirement of access control for critical resources [Section B - Physical Security of IT Infrastructure]



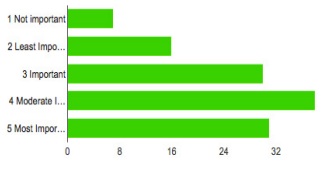
1 Not important	1	0.8%
2 Least Important	1	0.8%
3 Important	34	28.3%
4 Moderate Important	44	36.7%
5 Most Important	40	33.3%

Necessity of consolidated list of hardware inventory across the organization [Section C - Hardware & Software Security of IT Infrastructure]



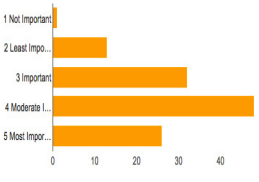
1 Not important	1	0.8%
2 Least Important	9	7.4%
3 Important	42	34.7%
4 Moderate Important	45	37.2%
5 Most Important	24	19.8%

Requirement of biometric authentication [Section B - Physical Security of IT Infrastructure]



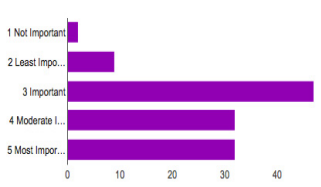
1 Not important	7	5.7%
2 Least Important	16	13.1%
3 Important	30	24.6%
4 Moderate Important	38	31.1%
5 Most Important	31	25.4%

Importance of deployment of adequate media destroy policy [Section C - Hardware & Software Security of IT Infrastructure]



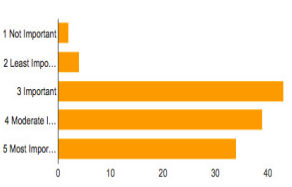
1 Not important	1	0.8%
2 Least Important	13	10.8%
3 Important	32	26.7%
4 Moderate Important	48	40%
5 Most Important	26	21.7%

Requirement of labelled removable computer media such as CDs,DATs,Tapes, DLTs etc. [Section C



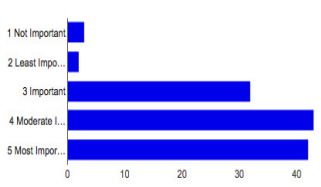
1 Not Important	2	1.6%
2 Least Important	9	7.4%
3 Important	47	38.5%
4 Moderate Important	32	26.2%
5 Most Important	32	26.2%

Proper labeling and classification of backup media. [Section D - Backup Security of IT Infrastructure]



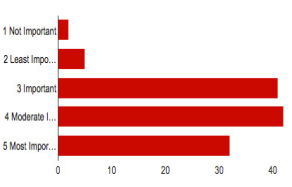
1 Not Important	2	1.6%
2 Least Important	4	3.3%
3 Important	43	35.2%
4 Moderate Important	39	32%
5 Most Important	34	27.9%

Security of media storage [Section C - Hardware & Software Security of IT Infrastructure]



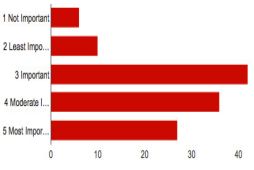
1 Not Important	3	2.5%
2 Least Important	2	1.6%
3 Important	32	26.2%
4 Moderate Important	43	35.2%
5 Most Important	42	34.4%

Maintenance of details of backup media by an organization [Section D - Backup Security of IT Infrastructure]



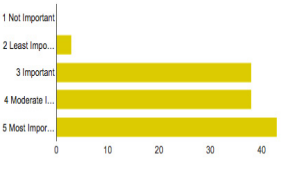
1 Not Important	2	1.6%
2 Least Important	5	4.1%
3 Important	41	33.6%
4 Moderate Important	42	34.4%
5 Most Important	32	26.2%

Maintenance records of all media that has been disposed off [Section C - Hardware & Software Security of IT Infrastructure]



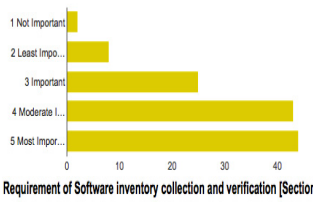
1 Not Important	6	5%
2 Least Important	10	8.3%
3 Important	42	34.7%
4 Moderate Important	36	29.8%
5 Most Important	27	22.3%

Security of the storage place of backup media [Section D - Backup Security of IT Infrastructure]



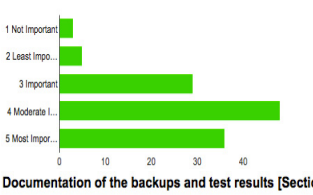
1 Not Important	0	0%
2 Least Important	3	2.5%
3 Important	38	31.1%
4 Moderate Important	38	31.1%
5 Most Important	43	35.2%

Requirement of separate ID cards for identification of vendor engineers deployed in the office [Section C



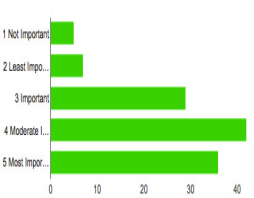
1 Not Important	2	1.6%
2 Least Important	8	6.6%
3 Important	25	20.5%
4 Moderate Important	43	35.2%
5 Most Important	44	36.1%

Implementation of backup retention policy in an organization. [Section D - Backup Security of IT Infrastructure]



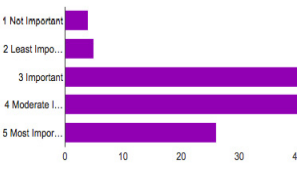
1 Not Important	3	2.5%
2 Least Important	5	4.1%
3 Important	29	24%
4 Moderate Important	48	39.7%
5 Most Important	36	29.8%

Requirement of Software inventory collection and verification [Section C - Hardware & Software Security of IT Infrastructure]



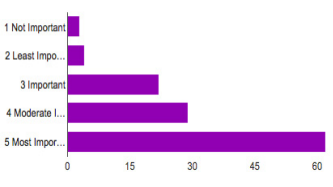
1 Not Important	5	4.2%
2 Least Important	7	5.9%
3 Important	29	24.4%
4 Moderate Important	42	35.3%
5 Most Important	36	30.3%

Documentation of the backups and test results [Section D - Backup Security of IT Infrastructure]



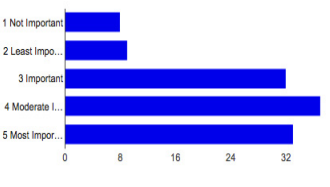
1 Not Important	4	3.3%
2 Least Important	5	4.1%
3 Important	44	36.1%
4 Moderate Important	43	35.2%
5 Most Important	26	21.3%

Use of license software [Section C - Hardware & Software Security of IT Infrastructure]



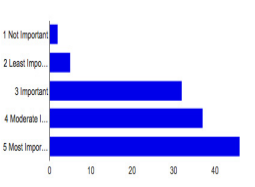
1 Not Important	3	2.5%
2 Least Important	4	3.3%
3 Important	22	18.3%
4 Moderate Important	29	24.2%
5 Most Important	62	51.7%

Requirement of BCP policy in an organization. [Section D - Backup Security of IT Infrastructure]



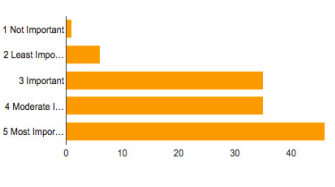
1 Not Important	8	6.7%
2 Least Important	9	7.6%
3 Important	32	26.9%
4 Moderate Important	37	31.1%
5 Most Important	33	27.7%

Requirement of security of storage of organization license software. [Section C - Hardware & Software Security of IT Infrastructure]

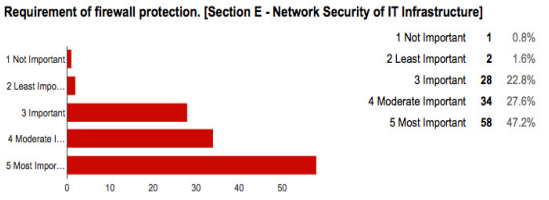


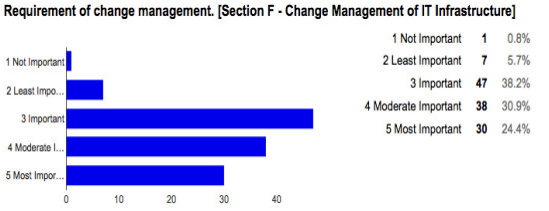
1 Not Important	2	1.6%
2 Least Important	5	4.1%
3 Important	32	26.2%
4 Moderate Important	37	30.3%
5 Most Important	46	37.7%

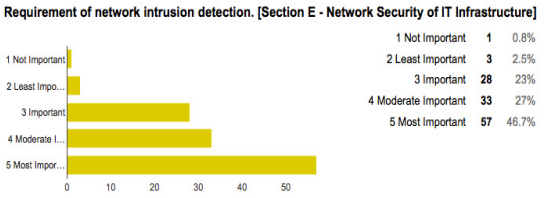
Requirement of router level security. [Section E - Network Security of IT Infrastructure]

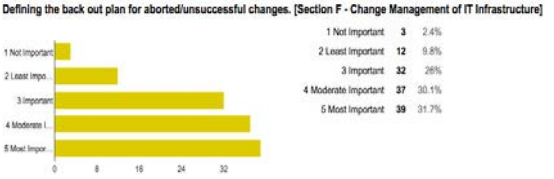


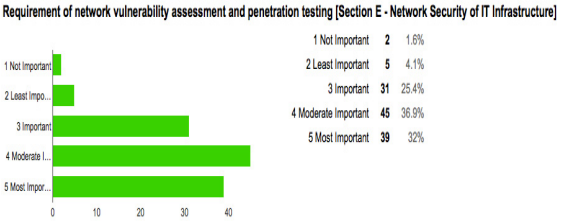
1 Not Important	1	0.8%
2 Least Important	6	4.9%
3 Important	35	28.5%
4 Moderate Important	35	28.5%
5 Most Important	46	37.4%

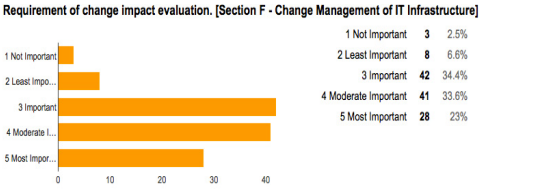


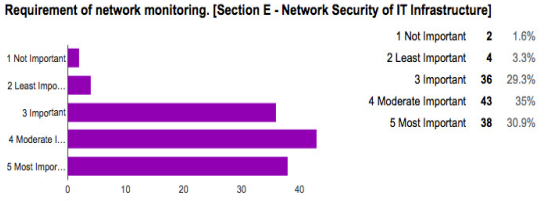


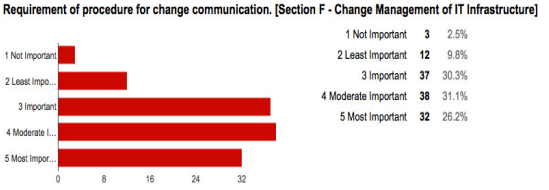












4. Discussion and conclusion

The growth of information security assessment usage increase the number of user using electronic services which leads to the need for the development of more efficient security assessment mechanisms, capable of assuring the protection of the user's information and identity, being at the same time adjusted to the needs of the market. Because IT infrastructure may not be completely incorporated into the business process and improved to perform efficiently and effectively in first place, which would have a substantial impact on control, quality and speed of information access, and the availability of information. Based on the responses of those who took part in the study, majority of students, faculty members, software worker favour the organization to have policies for Internet and IT infrastructure use and to also notify the users of the policies. It is believed that such policies and users awareness would reduce risks and liability. Though, a good number of the IT users who took part in this report indicated that they were not aware of such policies. Organizations have a vital part to show if IT users' interests are to be properly addressed. Organizations have to take main responsibilities in enlightening their IT users and in providing the necessary hardware and software that can enhance users' privacy and security. Thus in order to reap maximum benefits from any IT investments, the IT infrastructure must be optimized, benchmarked and its value to business quantifiable. That's why security plays an important role during the optimization process in bringing an IT infrastructure since a highly exposed state to an optimized state wherever a practice of continuous process improvements would ensure processes in place are mature and quantifiable. So the result of this survey highlights the focus areas and help significantly to proposed solution for enhancing IT infrastructure security evaluations.

References

1. Barr, C. (1998). CNET's privacy policy. CNET Personalities, http://www.cnet.com/Content/ Voices/Barr/040698/index.html, April.
2. Boswald, M., Hagin, C. and Markwiz, W. (1999). Methods and standards for privacy and authentication. in communications networks:[171] Godwin J. Udo Privacy and security concerns as major barriers for e-commerce: a survey study Information Management & Computer Security 9/4 [2001] 165±174 an overview'', International Journal of Electronics and Communications, June, p. 234.
3. csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.
4. EFF (1999) . Top 12 ways to protect your privacy. http://www.eff.org/pub/privacy/eff_privacy_top_12.html.
5. Federal Trade Commission (1999a). Information ± the currency of cyberspace. Site Seeing On the Internet, November, p. 2, http:// www.ftc.gov/bcp/conline/pubs/online/sitesee/.
6. Rubin, M.R. (1995) , Private Rights, Public Wrongs: The Computer and Personal Privacy, John Wiley and Sons, New York, NY.
7. Lehman, D. (2000). Protecting kids' privacy is costly. ComputerWorld, April, p. 97.
8. Martin, J. (1973) , Security, Accuracy, and Privacy in Computer Systems, Prentice-Hall, Englewood Cliffs, NJ.
9. Massey, A. (1999) . Privacy in the digital age. Houston Business Journal, Vol. 29 No. 50, p. 1b.
10. Moad, J. (1997) .Privacy issues surrounding the Internet. PC Week, October, p. 83. MSN wants to help you maintain your privacy on the Internet'', MSN.COM. Private Statement, p. 1, http://go.ms.com/.
11. Grandinetti, M. (1996) . Establishing and maintaining security on the Internet. Sacramento Business Journal, Vol. 13 No. 25, p. 22.
12. Black, M. C., Kresnow, M., Sim,on, T. R., Arisa, I., & Shelley, G. (2006). Telephone survey respondents' reactions to questions regarding interpersonal violence. Violence and Victims, 21(4), 445-459.
13. Morgan, S. D., & Roztocki, N. (2003). Web-based surveys as an academic research tool in engineering. IE Annual Conference Proceedings, 1.
14. Palys, T., & Lowman, J. (2002). Anticipating law: Research methods, ethics, and the law of privilege. Sociological Methodology, 32, 1-17.
15. Crespi, I. (1998). Ethical considerations when establishing survey standards. International Journal of Public Opinion Research, 10, 75-82.